

Konfigurieren des PPPoE-Clients auf einer Cisco Secure PIX Firewall

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Informationen zur Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Bekannte Probleme in PIX OS 6.2 und 6.3](#)

[Bekannte Probleme in PIX OS 6.3](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie der PPPoE-Client (Point-to-Point Protocol) auf der Cisco Secure PIX Firewall konfiguriert wird. PIX OS Version 6.2 führt diese Funktion ein und ist für Low-End-PIX (501/506) ausgelegt.

PPPoE kombiniert zwei weit verbreitete Standards, Ethernet und PPP, um eine authentifizierte Methode zur Zuweisung von IP-Adressen an Client-Systeme bereitzustellen. PPPoE-Clients sind in der Regel PCs, die über eine Remote-Breitbandverbindung, z. B. DSL oder Kabeldienst, mit einem ISP verbunden sind. ISPs stellen PPPoE bereit, da sie Hochgeschwindigkeits-Breitbandverbindungen über ihre vorhandene Remote-Zugriffsinfrastruktur unterstützen und die Verwendung für Kunden einfacher ist. PIX Firewall Version 6.2 führt PPPoE-Clientfunktionen ein. So können Benutzer in kleinen Büros und Heimbüros (SOHO) der PIX-Firewall mithilfe von DSL-Modems eine Verbindung zu ISPs herstellen.

Derzeit unterstützt nur die externe Schnittstelle des PIX diese Funktion. Sobald sich die Konfiguration auch auf der externen Schnittstelle befindet, wird der gesamte Datenverkehr mit PPPoE/PPP-Headern verkapselt. Der Standard-Authentifizierungsmechanismus für PPPoE ist Password Authentication Protocol (PAP).

PPPoE bietet eine Standardmethode zur Verwendung der Authentifizierungsmethoden des PPP über ein Ethernet-Netzwerk. Bei Verwendung durch ISPs ermöglicht PPPoE die authentifizierte

Zuweisung von IP-Adressen. Bei dieser Art der Implementierung sind der PPPoE-Client und der Server über Layer 2-Bridging-Protokolle verbunden, die über eine DSL- oder andere Breitbandverbindung ausgeführt werden.

Der Benutzer hat die Möglichkeit, Challenge Handshake Authentication Protocol (CHAP) oder MS-CHAP manuell zu konfigurieren. PIX OS 6.2 und 6.3 unterstützen das Layer 2 Tunneling Protocol (L2TP) und das Point-to-Point Tunneling Protocol (PPTP) mit PPPoE nicht.

PPPoE besteht aus zwei Hauptphasen:

- Aktive Erkennungsphase - In dieser Phase sucht der PPPoE-Client einen PPPoE-Server, den so genannten Zugriffskonzentrator. In dieser Phase wird eine Session-ID zugewiesen und die PPPoE-Ebene eingerichtet.
- PPP-Sitzungsphase - In dieser Phase werden PPP-Optionen ausgehandelt und eine Authentifizierung durchgeführt. Nach Abschluss der Verbindungseinrichtung fungiert PPPoE als Layer-2-Kapselungsmethode, sodass Daten über die PPP-Verbindung in PPPoE-Headern übertragen werden können.

Bei Systeminitialisierung richtet der PPPoE-Client eine Sitzung mit dem AC ein, indem er eine Reihe von Paketen austauscht. Nach Einrichtung der Sitzung wird eine PPP-Verbindung eingerichtet, die eine Authentifizierung mithilfe des PAP-Protokolls (Password Authentication) beinhaltet. Nach Einrichtung der PPP-Sitzung wird jedes Paket in die PPPoE- und PPP-Header gekapselt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX 501 mit PIX OS Version 6.3(4)
- Cisco 1721-Router mit Cisco IOS® Software Release 12.3(10), konfiguriert als PPPoE-Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt werden die Informationen vorgestellt, die Sie zum Konfigurieren der in diesem Dokument beschriebenen Funktionen verwenden können.

Hinweis: Um weitere Informationen zu den Befehlen zu erhalten, die dieses Dokument verwendet, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- [Cisco 1721 Router als PPPoE-Server](#)
- [PIX \(501 oder 506\) als PPPoE-Client](#)

In diesem Labortest fungiert ein Cisco 1721-Router als PPPoE-Server. Sie benötigen dies nicht in Ihrem Zuhause/Remote-Büro, da Ihr ISP den PPPoE-Server hostet.

Cisco 1721 Router als PPPoE-Server

```
!--- Username matches that on the PIX. username cisco
password cisco

!--- Enable virtual private dial-up network (VPDN). vpdn
enable
!

!--- Define the VPDN group that you use for PPPoE. vpdn-
group pppoex
  accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Ethernet0
  ip address 172.21.48.30 255.255.255.224
!--- Enable PPPoE sessions on the interface. pppoe
enable
!

interface Virtual-Template1
  mtu 1492
!--- Do not use a static IP assignment within a virtual
template since !--- routing problems can occur. Instead,
use the ip unnumbered command !--- when you configure a
virtual template.
```

```
ip unnumbered Ethernet0
peer default ip address pool pixpool
!--- Define authentication protocol. ppp authentication
pap
!
ip local pool pixpool 11.11.11.1 11.11.11.100
```

PIX (501 oder 506) als PPPoE-Client

```
pix501#write terminal
Building configuration...
: Saved
:
PIX Version 6.3(4)
interface ethernet0 10baset
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix501
domain-name cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Enable PPPoE client functionality on the interface.
!--- It is off by default. The setroute option creates a
default !--- route if no default route exists.

ip address outside pppoe setroute

ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.1.0 255.255.255.0 0 0
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
```

```

aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Define the VPDN group that you use for PPPoE. !---
Configure this first. vpdn group pppoe request dialout
pppoe

!--- Associate the username that the ISP assigns to the
VPDN group. vpdn group pppoe localname cisco

!--- Define authentication protocol. vpdn group pppoe
ppp authentication pap

!--- Create a username and password pair for the PPPoE
!--- connection (which your ISP provides). vpdn username
cisco password *****

terminal width 80
Cryptochecksum:e136533e23231c5bbbbf4088cee75a5a
: end
[OK]
pix501#

```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie die ordnungsgemäße Funktion Ihrer Konfiguration bestätigen können.

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show ip address outside pppoe**: Zeigt die aktuellen Konfigurationsinformationen des PPPoE-Clients an.
- **show vpdn tunnel pppoe**: Zeigt Tunnelinformationen für den jeweiligen Tunneltyp an.
- **show vpdn session pppoe**: Zeigt den Status von PPPoE-Sitzungen an.
- **show vpdn ppinterface**: Zeigt den Schnittstellenidentifizierungswert des PPPoE-Tunnels an. Für jeden PPPoE-Tunnel wird eine virtuelle PPP-Schnittstelle erstellt.
- **show vpdn group**: Zeigt die für den PPPoE-Tunnel definierte Gruppe an.
- **show vpdn username**: Zeigt die Informationen zum lokalen Benutzernamen an.

Dies ist die Ausgabe für den Befehl **show ip address outside pppoe**:

```
501(config)#show ip address outside pppoe
```

```
PPPoE Assigned IP addr: 11.11.11.1 255.255.255.255 on Interface: outside
Remote IP addr: 172.21.48.30
```

Dies ist die Ausgabe des Befehls **show vpdn tunnel pppoe**:

```
501(config)#show vpdn tunnel pppoe
```

```
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
```

```
Tunnel id 0, 1 active sessions  
time since change 20239 secs  
Remote MAC Address 00:08:E3:9C:4C:71  
3328 packets sent, 3325 received, 41492 bytes sent, 0 received
```

Dies ist die Ausgabe des Befehls **show vpdn session pppoe**:

```
501(config)#show vpdn session pppoe
```

```
PPPoE Session Information (Total tunnels=1 sessions=1)
```

```
Remote MAC is 00:08:E3:9C:4C:71  
Session state is SESSION_UP  
Time since event change 20294 secs, interface outside  
PPP interface id is 1  
3337 packets sent, 3334 received, 41606 bytes sent, 0 received
```

Dies ist die Ausgabe des Befehls **show vpdn pppinterface**:

```
501(config)#show vpdn pppinterface
```

```
PPP virtual interface id = 1  
PPP authentication protocol is PAP  
Server ip address is 172.21.48.30  
Our ip address is 11.11.11.1  
Transmitted Pkts: 3348, Received Pkts: 3345, Error Pkts: 0  
MPPE key strength is None  
MPPE_Encrypt_Pkts: 0, MPPE_Encrypt_Bytes: 0  
MPPE_Decrypt_Pkts: 0, MPPE_Decrypt_Bytes: 0  
Rcvd_Out_Of_Seq_MPPE_Pkts: 0
```

Dies ist die Ausgabe des Befehls **show vpdn group**:

```
501(config)#show vpdn group
```

```
vpdn group pppoex request dialout pppoe  
vpdn group pppoex localname cisco  
vpdn group pppoex ppp authentication pap
```

Dies ist die Ausgabe des Befehls **show vpdn username**:

```
501(config)#show vpdn username
```

```
vpdn username cisco password *****
```

[Fehlerbehebung](#)

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

[Informationen zur Fehlerbehebung](#)

Dies sind Beispieldbugs aus häufigen Fehlkonfigurationen auf dem PIX. Aktivieren Sie diese Debugger.

```
pix#show debug
debug ppp negotiation
debug pppoe packet
debug pppoe error
debug pppoe event
```

- Die Authentifizierung schlägt fehl (z. B. ungültiger Benutzername/Kennwort).

```
Rcvd Link Control Protocol pkt, Action code is: Echo Reply,
len is: 4 Pkt dump: d0c3305c
```

```
PPP pap rcv authen nak: 41757468656e74696361746966f6e2066661696c757265
PPP PAP authentication failed
```

```
Rcvd Link Control Protocol pkt, Action code is: Termination Request,
len is: 0
```

- Das Authentifizierungsprotokoll ist ungültig (z. B. PAP/CHAP falsch konfiguriert).

```
Xmit Link Control Protocol pkt, Action code is:
Config Request, len is: 6
```

```
Pkt dump: 05064a53ae2a
LCP Option: MAGIC_NUMBER, len: 6, data: 4a53ae2a
```

```
Rcvd Link Control Protocol pkt, Action code is: Config Request, len is: 14
```

```
Pkt dump: 010405d40304c0230506d0c88668
LCP Option: Max_Rcv_Units, len: 4, data: 05d4
LCP Option: AUTHENTICATION_TYPES, len: 4, data: c023
LCP Option: MAGIC_NUMBER, len: 6, data: d0c88668
```

```
Xmit Link Control Protocol pkt, Action code is: Config NAK, len is: 5
```

```
Pkt dump: 0305c22305
LCP Option: AUTHENTICATION_TYPES, len: 5, data: c22305
```

```
Rcvd Link Control Protocol pkt, Action code is: Config ACK, len is: 6
```

```
Pkt dump: 05064a53ae2a
LCP Option: MAGIC_NUMBER, len: 6, data: 4a53ae2a
```

- Der PPPoE-Server reagiert nicht, versuchen Sie es alle 30 Sekunden erneut.

```
send_padi:(Snd) Dest:ffff.ffff.ffff Src:0007.5057.e27e T
ype:0x8863=PPPoE-Discovery
```

```
Ver:1 Type:1 Code:09=PADI Sess:0 Len:12
Type:0101:SVNAME-Service Name Len:0
Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001
```

padi timer expired

```
send_padi:(Snd) Dest:ffff.ffff.ffff Src:0007.5057.e27e
Type:0x8863=PPPoE-Discovery
```

```
Ver:1 Type:1 Code:09=PADI Sess:0 Len:12
Type:0101:SVNAME-Service Name Len:0
Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001
```

padi timer expired

```
send_padi:(Snd) Dest:ffff.ffff.ffff Src:0007.5057.e27e
Type:0x8863=PPPoE-Discovery
```

```
Ver:1 Type:1 Code:09=PADI Sess:0 Len:12
Type:0101:SVNAME-Service Name Len:0
Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001
```

padi timer expired

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Lesen Sie [vor dem](#) Ausgabe von **Debug**-Befehlen unter [Wichtige Informationen zu Debug-Befehlen nach](#).

- **debug pppoe Packet:** Zeigt Paketinformationen an.
- **debug pppoe error (debug pppoe-Fehler):** Zeigt Fehlermeldungen an.
- **debug pppoe event (debug pppoe-Ereignis):** Zeigt Protokollereignisinformationen an.
- **debug ppp negotiation (PPP-Aushandlung debug)** - Ermöglicht Ihnen, zu sehen, ob ein Client PPP-Aushandlung-Informationen übergibt.
- **debug ppp io:** Zeigt die Paketinformationen für die virtuelle PPTP PPP-Schnittstelle an.
- **debug ppp upap:** Zeigt die PAP-Authentifizierung an.
- **debug ppp error (ppp-Fehler debuggen):** Zeigt Fehlermeldungen zur virtuellen PPTP-PPP-Schnittstelle an.
- **debug ppp chap:** Zeigt Informationen darüber an, ob ein Client die Authentifizierung durchläuft.

Verwenden Sie diese Befehle, um das Debuggen für den PPPoE-Client zu aktivieren:

```
!--- Displays packet information. 501(config)#debug pppoe packet

!--- Displays error messages. 501(config)#debug pppoe error

!--- Displays protocol event information. 501(config)#debug pppoe event

send_padi:(Snd) Dest:ffff.ffff.ffff Src:0008.a37f.be88 Type:0x8863=PPPoE-Discovery

  Ver:1 Type:1 Code:09=PADI Sess:0 Len:12

  Type:0101:SVCNAME-Service Name Len:0

  Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001

padi timer expired

PPPoE:(Rcv) Dest:0008.a37f.be88 Src:0008.e39c.4c71 Type:0x8863=PPPoE-Discovery

  Ver:1 Type:1 Code:07=PADO Sess:0 Len:45

  Type:0101:SVCNAME-Service Name Len:0

  Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001

  Type:0102:ACNAME-AC Name Len:9 3640

  Type:0104:ACCOOKIE-AC Cookie Len:16 D69B0AAF 0DEBC789 FF8E1A75 2E6A3F1B

PPPoE: PADO

send_padr:(Snd) Dest:0008.e39c.4c71 Src:0008.a37f.be88 Type:0x8863=PPPoE-Discovery
```



```
Ver:1 Type:1 Code:19=PADR Sess:0 Len:45
Type:0101:SVCNAME-Service Name Len:0
Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001
Type:0102:ACNAME-AC Name Len:9 3640
Type:0104:ACCOOKIE-AC Cookie Len:16 D69B0AAF 0DEBC789 FF8E1A75 2E6A3F1B
PPPoE:(Rcv) Dest:0008.a37f.be88 Src:0008.e39c.4c71 Type:0x8863=PPPoE-Discovery
Ver:1 Type:1 Code:65=PADS Sess:1 Len:45
Type:0101:SVCNAME-Service Name Len:0
Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001
Type:0102:ACNAME-AC Name Len:9 3640
Type:0104:ACCOOKIE-AC Cookie Len:16 D69B0AAF 0DEBC789 FF8E1A75 2E6A3F1B
```

PPPoE: PADS

IN PADS from PPPoE tunnel

PPPoE: Virtual Access interface obtained.PPPoE: Got ethertype=800
on PPPoE interface=outside

PPPoE: Got ethertype=800 on PPPoE interface=outside

PPPoE: Got ethertype=800 on PPPoE interface=outside

Diese Ausgabe enthält zusätzliche Debugbefehle für den PPPoE-Client:

```
501(config)#debug ppp negotiation
501(config)#debug ppp io
501(config)#debug ppp upap
501(config)#debug ppp error
```

PPP virtual access open, ifc = 0

```
Xmit Link Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 0506609b39f5
LCP Option: MAGIC_NUMBER, len: 6, data: 609b39f5
```

PPP xmit, ifc = 0, len: 14 data: ff03c0210101000a0506609b39f5

```
PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c02101010012010405d40304c023050659d9f636000000000000000000
00000000000000000000000000000000
```

```
Rcvd Link Control Protocol pkt, Action code is: Config Request, len is: 14
Pkt dump: 010405d40304c023050659d9f636
LCP Option: Max_Rcv_Units, len: 4, data: 05d4
LCP Option: AUTHENTICATION_TYPES, len: 4, data: c023
LCP Option: MAGIC_NUMBER, len: 6, data: 59d9f636
```

```
Xmit Link Control Protocol pkt, Action code is: Config ACK, len is: 14
Pkt dump: 010405d40304c023050659d9f636
LCP Option: Max_Rcv_Units, len: 4, data: 05d4
```


Rcvd IP Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 0306ac15301e
IPCP Option: Config IP, IP = 172.21.48.30

Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 030600000000
IPCP Option: Config IP, IP = 0.0.0.0

PPP xmit, ifc = 0, len: 14 data: ff0380210101000a030600000000

Xmit IP Control Protocol pkt, Action code is: Config ACK, len is: 6
Pkt dump: 0306ac15301e
IPCP Option: Config IP, IP = 172.21.48.30

PPP xmit, ifc = 0, len: 14 data: ff0380210201000a0306ac15301e

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210301000a03060b0b0b0200000000000000000000000000000000
00000000000000000000000000000000

Rcvd IP Control Protocol pkt, Action code is: **Config NAK**, len is: 6
Pkt dump: 03060b0b0b02
IPCP Option: Config IP, IP = 11.11.11.1

Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 03060b0b0b02
IPCP Option: Config IP, IP = 11.11.11.1

PPP xmit, ifc = 0, len: 14 data: ff0380210102000a03060b0b0b02

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210901000c59d9f636015995a1000000000000000000000000000000
00000000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Echo Request, len is: 8
Pkt dump: 59d9f636015995a1

Xmit Link Control Protocol pkt, Action code is: Echo Reply, len is: 8
Pkt dump: 609b39f5015995a1

PPP xmit, ifc = 0, len: 16 data: ff03c0210a01000c609b39f5015995a1

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210202000a03060b0b0b0200000000000000000000000000000000
00000000000000000000000000000000

Rcvd IP Control Protocol pkt, Action code is: Config ACK, len is: 6
Pkt dump: 03060b0b0b02
IPCP Option: Config IP, IP = 11.11.11.1

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210902000c59d9f6360159937b000000000000000000000000000000
00000000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Echo Request, len is: 8
Pkt dump: 59d9f6360159937b

Xmit Link Control Protocol pkt, Action code is: Echo Reply, len is: 8
Pkt dump: 609b39f50159937b

PPP xmit, ifc = 0, len: 16 data: ff03c0210a02000c609b39f50159937b

Xmit Link Control Protocol pkt, Action code is: Echo Request, len is: 4
Pkt dump: 609b39f5

Pkt dump: 3ff50e18

PPP xmit, ifc = 0, len: 12 data: ff03c021090000083ff50e18

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c2230103001508bfe11df6d8fb5243333634302020202000000000000
0000000000000000000000000000

PPP chap receive challenge: rcvd a type MS-CHAP-V1 pkt

PPP xmit, ifc = 0, len: 63 data:
ff03c2230203003b31488506adb9ae0f4cac35866242b2bac2863870291e4a88e1458f0
12526048734778a210325619092d3f831c3bcf3eb7201636973636f

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210a00000859f4cf2500
0000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Echo Reply, len is: 4
Pkt dump: 59f4cf25

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c2230303000400
0000000000000000000000000000

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210101000a0306ac15301e000000000000000000000000000000000000
0000000000000000000000000000

Rcvd IP Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 0306ac15301e
IPCP Option: Config IP, IP = 172.21.48.30

Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 030600000000
IPCP Option: Config IP, IP = 0.0.0.0

PPP xmit, ifc = 0, len: 14 data: ff0380210101000a030600000000

Xmit IP Control Protocol pkt, Action code is: Config ACK, len is: 6
Pkt dump: 0306ac15301e
IPCP Option: Config IP, IP = 172.21.48.30

PPP xmit, ifc = 0, len: 14 data: ff0380210201000a0306ac15301e

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210301000a03060b0b0b02000000000000000000000000000000000000
0000000000000000000000000000

Rcvd IP Control Protocol pkt, Action code is: Config NAK, len is: 6
Pkt dump: 03060b0b0b02
IPCP Option: Config IP, IP = 11.11.11.1

Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 03060b0b0b02
IPCP Option: Config IP, IP = 11.11.11.1

PPP xmit, ifc = 0, len: 14 data: ff0380210102000a03060b0b0b02

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210202000a03060b0b0b02000000000000000000000000000000000000
0000000000000000000000000000

Rcvd IP Control Protocol pkt, Action code is: Config ACK, len is: 6
Pkt dump: 03060b0b0b02

IPCP Option: Config IP, IP = 11.11.11.1

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210901000c59f4cf2501592b7e00000000000000000000000000000000
00000000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Echo Request, len is: 8
Pkt dump: 59f4cf2501592b7e

Xmit Link Control Protocol pkt, Action code is: Echo Reply, len is: 8
Pkt dump: 3ff50e1801592b7e

PPP xmit, ifc = 0, len: 16 data: ff03c0210a01000c3ff50e1801592b7e

Xmit Link Control Protocol pkt, Action code is: Echo Request, len is: 4
Pkt dump: 3ff50e18

PPP xmit, ifc = 0, len: 12 data: ff03c021090100083ff50e18

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210a01000859f4cf2500
00000000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Echo Reply, len is: 4
Pkt dump: 59f4cf25

[Bekannte Probleme in PIX OS 6.2 und 6.3](#)

- Wenn die Standardroute bereits konfiguriert ist, stellt PIX das PPPoE nicht her, da es die vorhandene Standardroute nicht mit der Standardroute überschreiben kann, die das PPPoE bereitstellt. Wenn Sie die Standardroute vom Server (**setroute**-Option) verwenden möchten, muss der Benutzer die Standardroute in der Konfiguration löschen.
- Sie definieren nur einen Benutzernamen und einen PPPoE-Server.

[Bekannte Probleme in PIX OS 6.3](#)

- Wenn Sie PPPoE und Open Shortest Path First (OSPF) aktivieren und **Arbeitsspeicher** nach dem Abruf einer IP-Adresse ausgeführt wird, wird die heruntergeladene Standardroute über PPPoE oder DHCP in der Konfiguration gespeichert. Die Problemumgehung besteht darin, **Schreibspeicher** auszuführen, bevor die Adresse vom PPPoE-Server heruntergeladen wird.
- Die PPPoE **setroute**-Option, mit der Sie eine Standardroute generieren, ist nicht mit dem dynamischen OSPF-Routing-Protokoll der PIX Firewall kompatibel. Die vom PPPoE erzeugte Standardroute wird aus der Routing-Tabelle entfernt, wenn die "Netzwerk"-Anweisung im Rahmen des OSPF-Prozesses konfiguriert wird. Die Lösung besteht darin, statische Routen zu verwenden.

[Zugehörige Informationen](#)

- [PIX-Support-Seite](#)
- [PIX-Befehlsreferenz](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)